Kazakhstan DMARC Adoption Report 2023

POWERDMARC

POWERDMARC

Case study

Why is Increasing DMARC Adoption in Kazakhstan Essential?

- Boosting the adoption and correct deployment of DMARC in Kazakhstan is an important step toward furthering the security of the country's online defenses. It's a proactive step to keep our digital world safe now and in the future. As cyber attacks increase, Kazakhstani organizations need to do more to stop harmful emails from getting through and harming their customers.
- By using email authentication tools like DMARC, Kazakhstan's organizations can show they're serious about protecting their emails. This not only makes them appear as credible sources but also keeps their information safe. This is really crucial for financial establishments like banks, government offices, hospitals, and schools that send private information through emails, along with any organization dealing with sensitive data.

Is Kazakhstan Adequately Protected Against Email Fraud?

- In the first half of 2021, the Kazakh computer security team, KZ-CERT, dealt with a whopping 11,432 cases of cyber threats. That's a 15% jump compared to last year.
- Businesses, governmental establishments, and unsuspecting individuals have all been on the attacker's hit list. As reported on August 2021, no bank in Kazakhstan could prove they had strong security measures in place needed to safeguard their websites, data, or emails from cyberattacks. The state government recognized that the reason for these drawbacks was the lack of education and awareness against information and communication security, especially among small and mid-sized businesses in Kazakhstan.
- In May of 2023, Ukraine's computer emergency response team, known as CERT-UA, detected a cyber-espionage operation directed at an undisclosed Ukrainian government agency.
- Researchers pinpointed a threat actor labeled as UAC-0063, which exhibited indications of intent to focus on countries including Mongolia, Kazakhstan, Kyrgyzstan, Israel, and India. Attack vectors and modes of deployment included compromised email accounts and email phishing scams.

- The above-mentioned statistics highlight the potential threat to email and information systems in Kazakhstan, and the immediate need to be proactive.

In this report, we focussed on answering the following questions:

- What is the current situation of DMARC adoption and enforcement in organizations in Kazakhstan?
- How can we improve the cybersecurity and email authentication infrastructure in Kazakhstan to mitigate impersonation attacks?

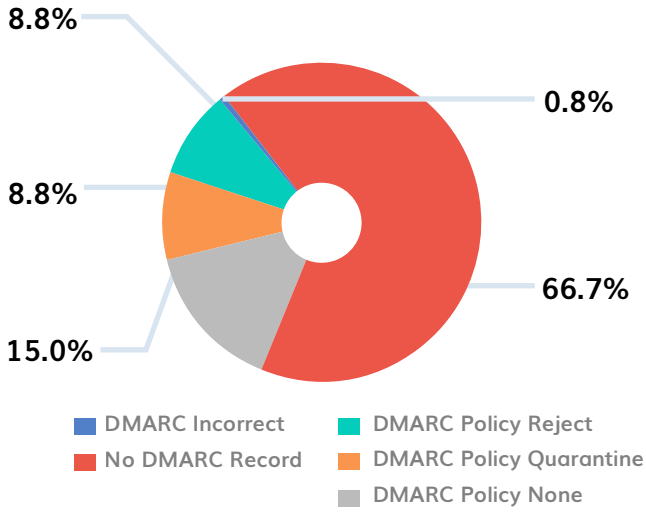
To gain better insight into the current scenario we analyzed 525 domains belonging to top businesses and organizations in Kazakhstan, from the following sectors:

- Healthcare
- Energy
- Government
- Banking
- Educational
- Telecom
- Media
- Transport

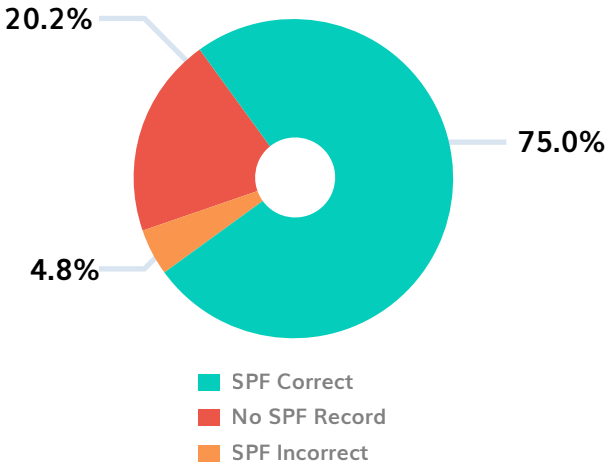
What Do the Numbers Say?

An in-depth SPF and DMARC adoption analysis was conducted while examining all 525 Kazakhstani domains, which led to the following revelations:

DMARC Adoption Analysis in Uzbekistan



SPF Adoption Analysis in Uzbekistan

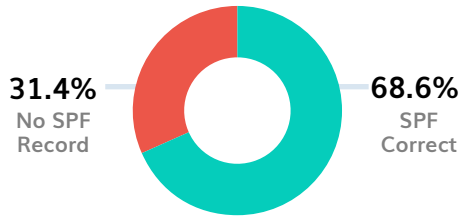


- Graphical Analysis: Among all 525 domains examined that belong to various organizations in Kazakhstan, 394 domains (75%) possessed correct SPF records, while 106 domains (20.2%) unfortunately had no SPF records at all, and 25 domains (4.8%) had incorrect records.
  A vast majority of domains (350 domains making up 66.7%) had no DMARC records at all. 79 domains had their DMARC policy set at none (15%), enabling monitoring only, while 46 domains (8.8%) had their DMARC policy level set at quarantine, and 46 domains (8.8%) had their DMARC policy set at maximum enforcement (i.e. p=reject).

Sector-wise Analysis of Kazakhstani Domains

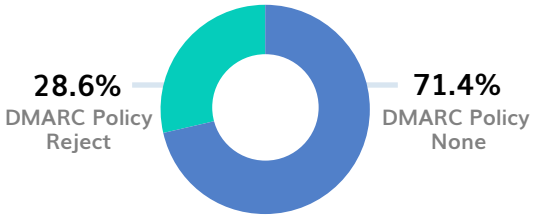
Healthcare Sector

SPF Adoption Analysis: Healthcare Sector



DMARC Adoption Analysis: Healthcare Sector

DMARC Enforcement Rates: Healthcare Sector

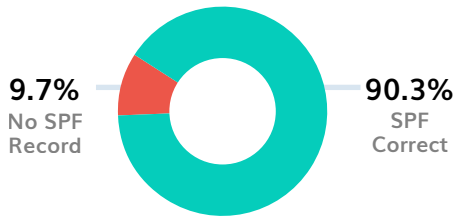


Key Findings:

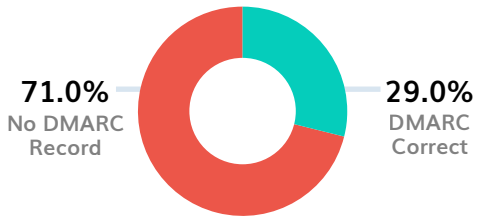
- 31.4% of domains in the Kazakhstan Telecom sector had no SPF record
- 71.4% of DMARC-implemented domains were at p=none offering no protection
- No DMARC record was found for 80% of the domains

Energy Sector

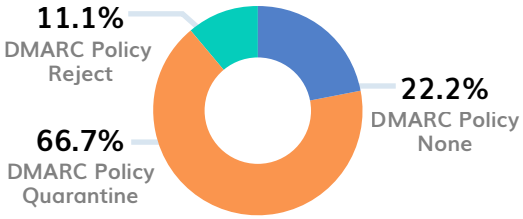
SPF Adoption Analysis: Energy Sector



DMARC Adoption Analysis: Energy Sector



DMARC Enforcement Rates: Energy Sector

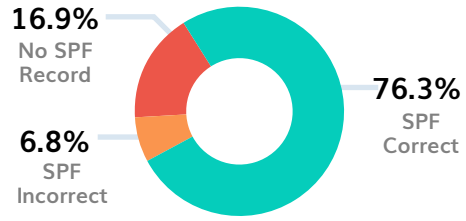


Key Findings:

- 9.7% of the domains had no SPF record published in their DNS
- 71% of the domains had no DMARC record published in their DNS
- 22.2% of the domains with DMARC implemented were on a “none” policy

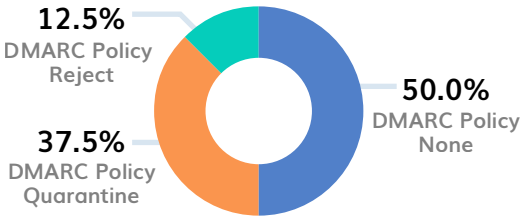
Government Sector

SPF Adoption Analysis: Government Sector



DMARC Adoption Analysis: Government Sector

DMARC Enforcement Rates: Government Sector

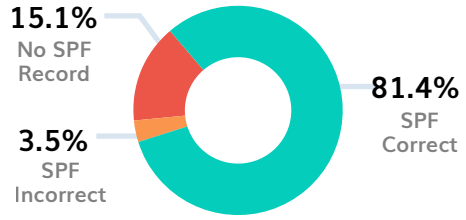


Key Findings:

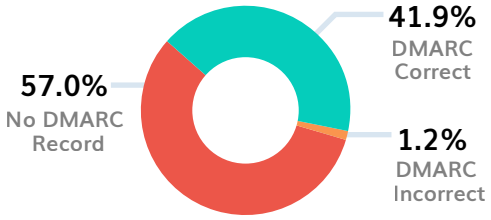
- 16.9% of the domains had no SPF record published in their DNS
- 72.9% of the domains had no DMARC record published in their DNS
- 50% of the domains with DMARC implemented were on a “none” policy

Banking Sector

SPF Adoption Analysis: Banking Sector



DMARC Adoption Analysis: Banking Sector



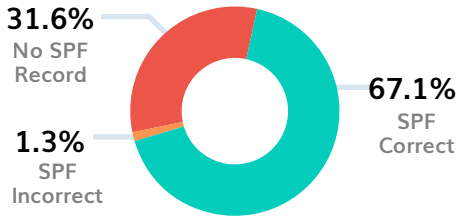
DMARC Enforcement Rates: Banking Sector

Key Findings:

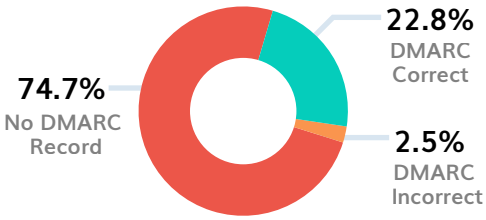
- 15.1% of the domains had no SPF record published in their DNS
- 57% of the domains had no DMARC record published in their DNS
- 30.6% of the domains with DMARC implemented were on a “none” policy

Educational Sector

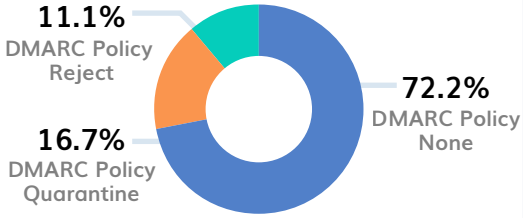
SPF Adoption Analysis: Education Sector



DMARC Adoption Analysis: Education Sector



DMARC Enforcement Rates: Education Sector

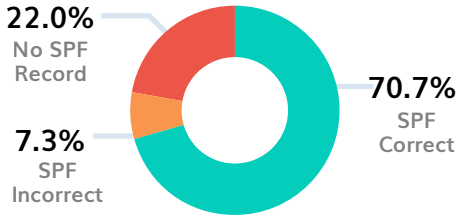


Key Findings:

- 31.6% of the domains had no SPF record published in their DNS
- 74.7% of the domains had no DMARC record published in their DNS
- 72.2% of the domains with DMARC implemented were on a “none” policy

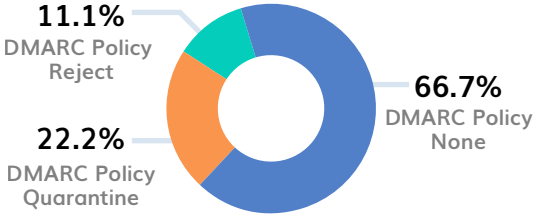
Telecom Sector

SPF Adoption Analysis: Telecom Sector



DMARC Adoption Analysis: Telecom Sector

DMARC Enforcement Rates: Telecom Sector

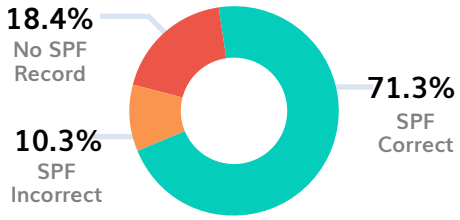


Key Findings:

- 22% of the domains had no SPF record published in their DNS
- 56.1% of the domains had no DMARC record published in their DNS
- 66.7% of the domains with DMARC implemented were on a “none” policy

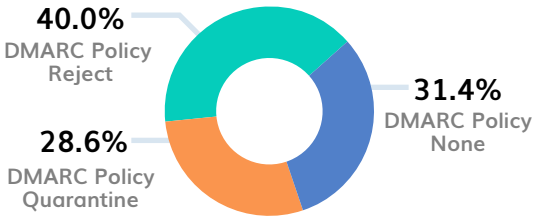
Media & Entertainment Sector

SPF Adoption Analysis: Media and Entertainment Sector



DMARC Adoption Analysis: Media and Entertainment Sector

DMARC Enforcement Rates: Media and Entertainment Sector

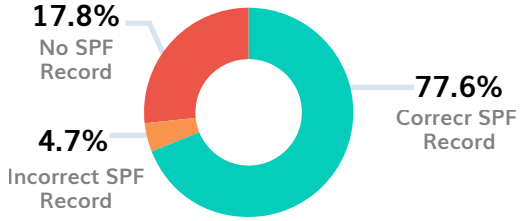


Key Findings:

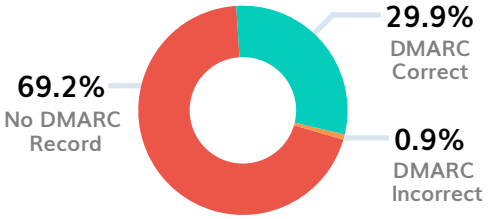
- 18.4% of the domains had no SPF record published in their DNS
- 59.8% of the domains had no DMARC record published in their DNS
- 31.4% of the domains with DMARC implemented were on a “none” policy

Transport Sector

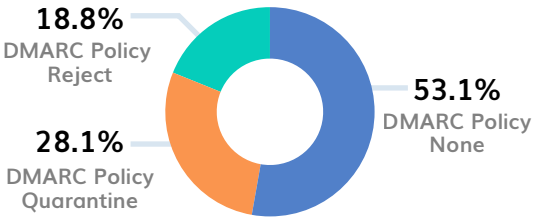
SPF Adoption Analysis: Telecom Sector



DMARC Adoption Analysis: Telecom Sector



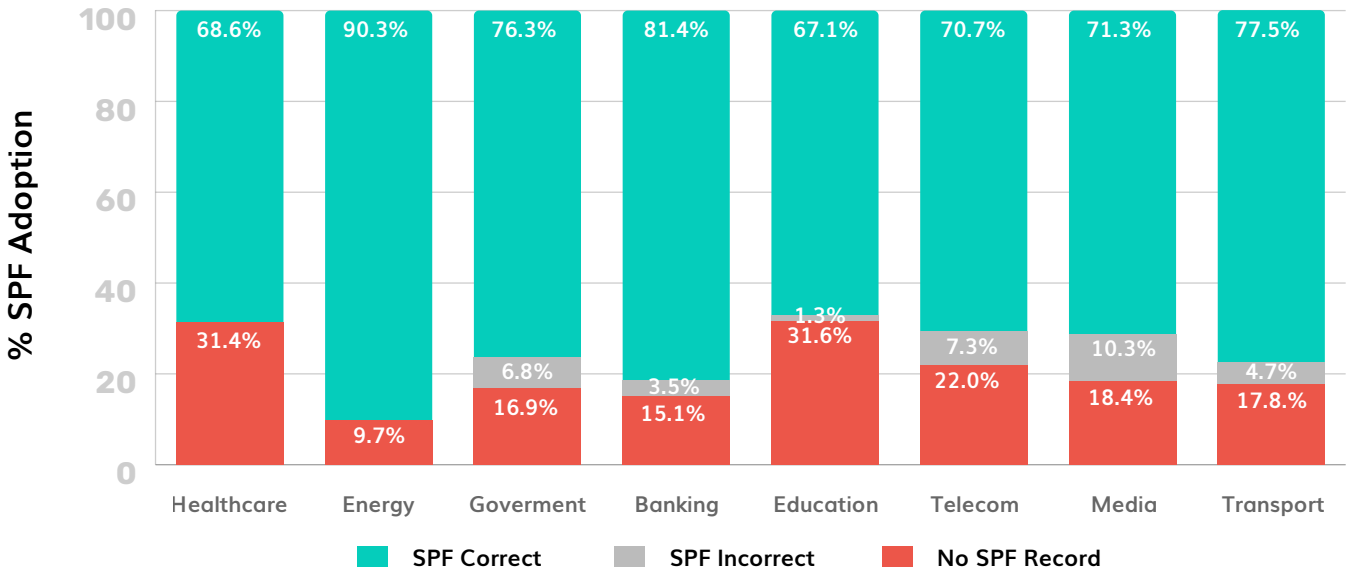
DMARC Enforcement Rates: Transport Sector



Key Findings:

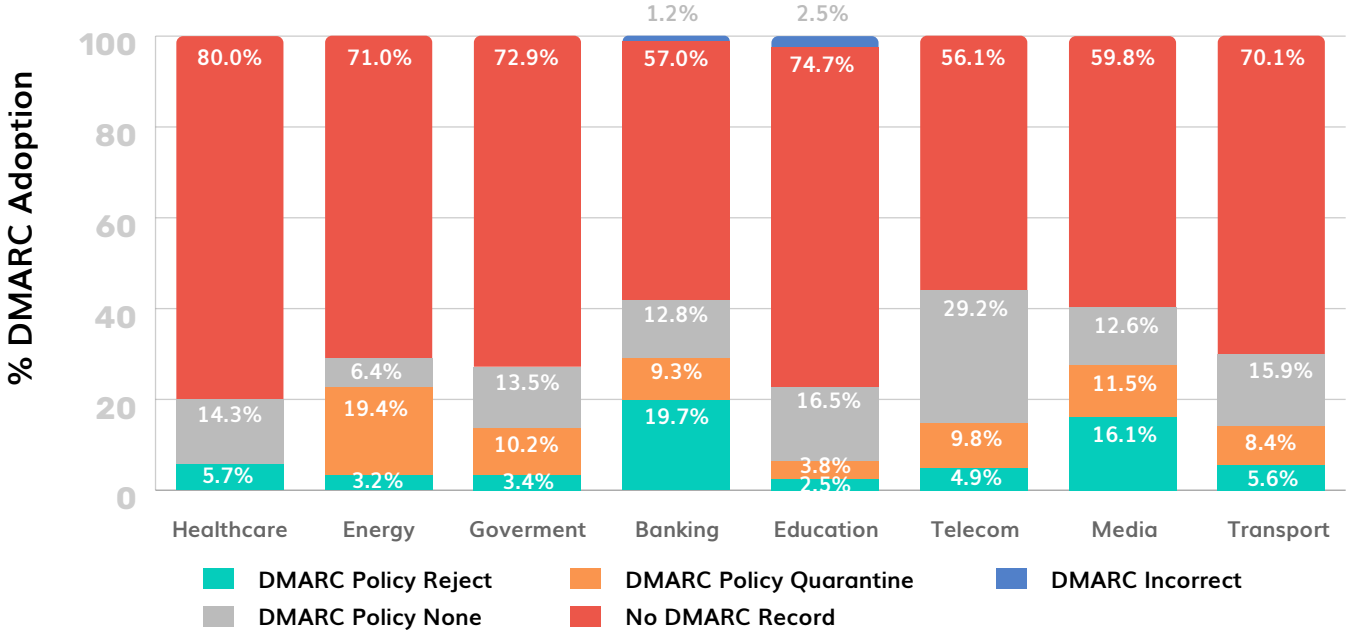
- 17.8% of the domains had no SPF record published in their DNS
- 69.2% of the domains had no DMARC record published in their DNS
- 53.1% of the domains with DMARC implemented were on a “none” policy

Comparative Analysis of SPF Adoption among Different Sectors in Kazakhstan



The SPF adoption rate was found to be **the lowest** in the Kazakhstan **educational** and **healthcare sector**. The highest rate of SPF adoption was noted in the Kazakhstani **energy, government,** and **banking sector.**

Comparative Analysis of DMARC Adoption among Different Sectors in Kazakhstan



The Kazakhstan **healthcare sector** noted the **lowest rate** of DMARC adoption. The **highest rate** of DMARC adoption was noted among **telecom, banking,** and **media & entertainment** sectors however with considerably low rates of enforcement. A large percentage of organizations in all sectors had their DMARC policies at **monitoring only.**

Where are Organizations in Kazakhstan Going Wrong?

Upon reviewing 525 domains registered in Kazakhstan spanning various sectors and industries, it becomes evident that organizations operating within the country are making noteworthy errors that might potentially jeopardize the security of email communications shared with their clients or employees.

SPF and DMARC Records are Not Correct

In the event that your email server employs incorrect SPF or DMARC record syntax, there's a chance that your genuine emails could be diverted to the spam folder or get outright rejected by the recipient's email service provider. This can potentially harm your email's credibility and also lead recipients to question the authenticity of your messages. This, in turn, can impact your overall email deliverability rates.

Low Support for Email Authentication

A concerning number of domains in Kazakhstan lacks the implementation of email authentication protocols like SPF and DMARC. These mechanisms function as protective barriers for your email domain. The complete absence of these measures creates an opportunity for hackers to impersonate your emails, potentially deceiving individuals into divulging sensitive information.

Excessive DNS Queries for SPF

The RFC mandates a ceiling of 10 SPF lookups. Crossing this threshold with excessive DNS requests can result in complications and render your SPF configuration ineffective.

DMARC Policy Offering Zero Protection

It's a popular myth that even with a p=none DMARC policy you're adequately protected against email-based attacks. In reality, if your DMARC policy is not set to "reject" or "quarantine," scammers can continue to send emails that mimic the appearance of originating from your domain. These emails might reach your clients without obstruction or being labeled as spam, thereby increasing the likelihood of successful phishing endeavors.

Absence of MTA-STS Integration

MTA-STS serves as a safeguard for your emails during transmission, preventing unauthorized access and manipulation by hackers. Failing to incorporate this protection could leave your email system susceptible to vulnerabilities.

Plurality of SPF Records for a Single Domain

For your domain, it's advisable to maintain a singular SPF record. The presence of multiple records can lead to challenges in email authentication.

Methods to Improve Email Security in Kazakhstan

- Kazakhstani organizations can take the following steps to improve their overall email security posture:

1. Securing your domains against impersonation via enforced DMARC policies
2. Maintaining SPF within the 10 DNS lookup limit
3. Ensuring error-free SPF and DMARC records
4. Employing a singular SPF/DMARC record per domain
5. Deploying MTA-STS, and TLS-RPT to thwart attacks like Man-in-the-Middle
6. Activating BIMI for enhanced visibility and authentication

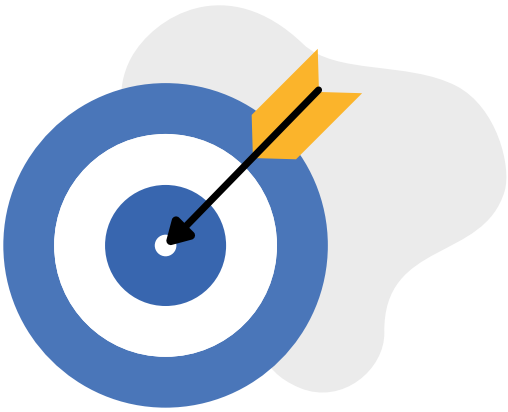
Benefits of PowerDMARC for Your Email Security Enhancement

Creating a secure email environment necessitates the activation of email authentication protocols—DMARC, DKIM, SPF, MTA-STS, TLS-RPT, and BIMI—across all domains within your company. This standardizes security measures for internal communications and guards against inadvertent or malicious sources.

PowerDMARC provides an extensive range of email security solutions to safeguard your brand reputation and shield customers from email-related threats. Our services simplify the intricate process of protocol setup, management, and monitoring.

Here's what we offer:

- **Configuration:** We aid in establishing and validating SPF, DKIM, and DMARC records through our hosted services, ensuring their effectiveness and correctness.
- **Setup:** Our DMARC trial facilitates the creation of your DMARC dashboard, offering visibility within a mere 72 hours of sign-up.
- **Monitoring:** Round-the-clock monitoring of email traffic identifies and handles security incidents, supplemented by alerts, reports, and responsive measures for managing legitimate sources.
- **Reporting:** Daily Aggregate (RUA) and Forensic (RUF) reports provide insight into DMARC status for your domains, with readable formats, actionable buttons, charts, and filtering choices. Aggregate reports are downloadable in PDF/CSV formats.
- **Enforcement:** We guide you through DMARC enforcement, securely transitioning to "p=reject/quarantine" policies.
- **PowerSPF:** Our instant and automated SPF flattening service maintains DNS lookup limits, with real-time updates on ESP changes.
- **Advanced Authentication Protocols:** Leveraging MTA-STS, TLS-RPT, and BIMI in conjunction with standard protocols effectively addresses email security concerns.
- **Domain Security Analysis Tools:** Access instant analysis tools for domain security ratings, email headers, domain health scores, and actionable recommendations for ongoing improvement and defense strengthening.
- **Managed Security Services:** Our DMARC MSSP/MSP-ready platform features a dedicated service desk, supporting DMARC implementation and domain health monitoring with white-label and multi-tenancy support.



Partnering with PowerDMARC bolsters your email domains and customer protection, ensuring secure and reliable communication for your organization and clients, and mitigating potential threats.

Let's join hands to increase the rate of DMARC adoption and strengthen the email security infrastructure in businesses across Kazakhstan. Get in touch with us at sales@powerdmarc.com to find out how we can help protect your domain and business today!

Contact us!